IN THE CLAIMS

PLEASE AMEND THE CLAIMS AS FOLLOWS:

1. (currently amended) A method for classifying a message, comprising:
   extracting a plurality of reference points from a body of the message, each reference point being information used to contact a referenced entity;
   classifying each of the plurality of reference points based on a source associated with each reference point; ~~and~~
   ~~detecting that~~ determining whether the message is a ~~phish~~ fraudulent message appearing to be from a legitimate source based on the classified reference points; and
   processing the message based on the determination of whether the message is a ~~phish~~ fraudulent message appearing to be from a legitimate source.

2. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, wherein classifying the plurality of reference points ~~including~~ includes looking up the plurality of reference points in a database.

3. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, wherein detecting that the message is a ~~phish~~ fraudulent message appearing to be from a legitimate source includes determining that the message includes divergent reference points.

4. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, wherein detecting that the message is a ~~phish~~ fraudulent message appearing to be from a legitimate source includes determining that the plurality of reference points includes a first reference point to a first source and a second reference point to a second source.

5. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, wherein detecting that the message is a ~~phish~~ fraudulent message appearing to be from a legitimate source includes determining that the plurality of reference points includes a first reference point to a legitimate source and a second reference point to a questionable search.

6. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, wherein detecting that the message is a ~~phish~~ fraudulent message appearing to be from a legitimate source includes determining that the plurality of reference points includes a first reference point to a first source and a second reference point to a second source, and the second reference point is intended to appear as a reference to the first source.

7. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, further comprising computing a thumbprint of the message and storing the thumbprint to a database.

8. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, further comprising computing a thumbprint of the message and storing the thumbprint to a database; wherein the database is shared.

9. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, further comprising identifying a plurality of fraud indicators and applying a statistical analysis on the plurality of fraud indicators.

10. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, further comprising quarantining the message.

11. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, further comprising deleting the message.

12. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, further comprising providing an alert to a recipient of the message.

13. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, further comprising providing an alert to a recipient indicating that the message is a ~~phish~~ fraudulent message appearing to be from a legitimate source.

14. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 1, further comprising providing an explanation of the ~~phish~~ fraudulent message appearing to be from a legitimate source to a recipient.

15. (currently amended) A method for classifying a message, comprising:

identifying a plurality of fraud indicators in the message;

applying a statistical analysis on the plurality of fraud indicators; ~~and~~

determining whether the message is a fraudulent message based on the analysis; and

processing the message based on the determination of whether the message is a fraudulent message.

16. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 15, wherein identifying the plurality of fraud indicators includes identifying a raw Internet protocol (IP) address.

17. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 15, wherein identifying the plurality of fraud indicators includes identifying non-standard encoding in the message.

18. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 15, wherein identifying the plurality of fraud indicators includes identifying a link with an embedded user name.

19. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 15, wherein identifying the plurality of fraud indicators includes identifying a misleading link.

20. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 15, wherein identifying the plurality of fraud indicators includes identifying a mismatched link name.

21. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 15, wherein identifying the plurality of fraud indicators includes identifying a form in the message.

22. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 15, wherein identifying the plurality of fraud indicators includes identifying a form tin the message that requests special information.

23. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 15, wherein identifying the plurality of fraud indicators includes identifying suspect content in the message.

24. (currently amended) ~~A~~ The method ~~for classifying a message as recited in Claim~~ of claim 15, wherein applying a statistical analysis on the plurality of fraud indicators includes obtaining a score based on the fraud indicators.

25. (cancelled)

26. (currently amended) A computer readable storage medium having embodied thereon a program ~~product~~ , the program being executable by a processor to perform a method for classifying a message, the ~~computer program product being embodied in a computer readable medium and comprising computer instructions for~~ the method comprising:

extracting a plurality of reference points from a body of the message;

classifying the plurality of reference points; ~~and~~

~~detecting that~~ determining whether the message is a ~~phish~~ fraudulent message appearing to be from a legitimate source based on the classified reference points; and

processing the message based on the determination of whether the message is a ~~phish~~ fraudulent message appearing to be from a legitimate source.

27. (cancelled)

28. (currently amended) A computer readable storage medium having embodied thereon a program ~~product~~ , the program being executable by a processor to perform a method for classifying a message, ~~the computer program product being embodied in a computer readable medium and comprising computer instructions for~~ the method comprising:

identifying a plurality of fraud indicators in the message;

applying a statistical analysis on the plurality of fraud indicators; ~~and~~

determining whether the message is a fraudulent message based on the analysis; and

processing the message based on the determination of whether the message is a fraudulent message.